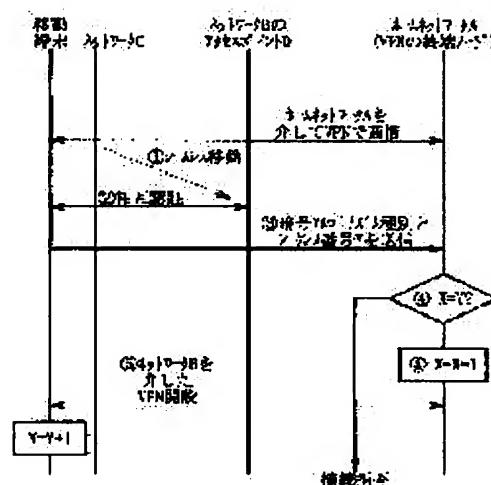


(11)Publication number : 2000-244547  
(43)Date of publication of application : 08.09.2000

(72)Inventor : KUNO YUTAKA  
HANAZAWA TETSUO  
MORIKURA MASAHIRO

**SOLUTION:** On the basis of network information reported from an access network B, a mobile terminal judges the strength of a required cipher and select the encryption algorithm. Afterwards, at the time of certification with the tunnel server of a home network A, the mobile terminal sends the class of the selected encryption algorithm and information capable of specifying this session while signing with the signature key thereof. The tunnel server verifies that signature and after the information capable of specifying this session reported from the mobile terminal is collated with information capable of specifying this session managed by the tunnel server, enciphered VPN communication based on the selected encryption algorithm is started.



(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-244547

(P2000-244547A)

(43) 公開日 平成12年9月8日(2000.9.8)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ターミナル <sup>*</sup> (参考)
H 0 4 L 12/46		H 0 4 L 11/00	3 1 0 C 5 J 1 0 4
		G 0 9 C 1/00	6 6 0 E 5 K 0 3 0
G 0 9 C 1/00	6 6 0	H 0 4 L 9/00	6 4 1 5 K 0 3 3
H 0 4 L 9/14			6 7 1 9 A 0 0 1
9/32		11/20	B

審査請求 未請求 請求項の数 6 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願平11-39196

(22) 出願日 平成11年2月17日(1999.2.17)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 久埜 豊

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(72) 発明者 花澤 徹郎

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

(74) 代理人 100064908

弁理士 志賀 正武

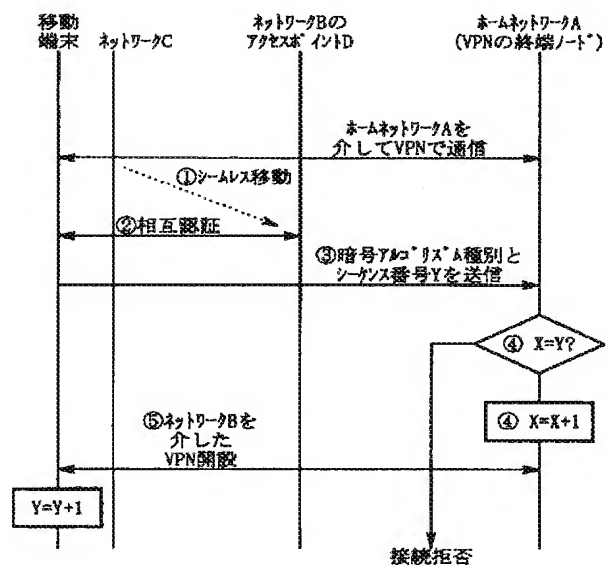
最終頁に続く

## (54) 【発明の名称】 認証方法

## (57) 【要約】

【課題】 異種ネットワーク間で移動しながらホームネットワークへのアクセスを継続しても、適切な暗号化アルゴリズムを選択できること。

【解決手段】 移動端末は、アクセスネットワークBより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択する。その後、移動端末は、ホームネットワークAのトンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定する情報とを、自分の署名鍵で署名して送出する。トンネルサーバーは、該署名を検証し、移動端末より通知された今回のセッションを特定する情報とトンネルサーバーが管理している今回のセッションを特定する情報とを照合した上で、選択された暗号化アルゴリズムによる暗号化されたVPN通信を開始する。



## 【特許請求の範囲】

【請求項1】 移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネットワークとの接続時に認証を行い、アクセスネットワークとの認証時に、アクセスネットワークより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、トンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定しうる情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、正当性が認識されると、選択された暗号化アルゴリズムによる暗号化されたVPN通信を開始することを特徴とする認証方法。

【請求項2】 請求項1記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする認証方法。

【請求項3】 請求項1記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする認証方法。

【請求項4】 移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネットワークとの接続時に認証を行い、トンネルサーバーとの認証時に、今回のセッションを特定しうる情報とアクセスネットワークとの認証時にアクセスネットワークより通知されたネットワーク情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる

情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、

正当性が認識されると、移動端末より通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、選択された暗号化アルゴリズムによる暗号化されたVPN通信を開始することを特徴とする認証方法。

【請求項5】 請求項4記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする認証方法。

【請求項6】 請求項4記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする認証方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、異種ネットワーク間でシームレス移動を行いながらホームネットワークへアクセスする場合における認証方法に関する。

【0002】

【従来の技術】近年、モバイル・コンピューティングの進展に従い、ファイアウォール(firewall)を越えて、自分が平常アクセスしているオフィスのネットワークに、外部からアクセスするVPN(Virtual Private Network)技術が発展を見ている。VPNの根幹は、ファイアウォール内にあるトンネルサーバーによる認証と暗号化トンネルの開設である。

【0003】図3は、VPNを開設しながら、移動端末がアクセスネットワーク(構内ネットワーク)B、Cを介してホームネットワークAに外部からアクセスを行うシステムの概要例を示す説明図である。この図において、ファイアウォールは、トンネルサーバーとの認証パケット、及び、トンネルサーバーとの暗号化トンネルを通るパケットのみを通すように設定されている。

【0004】暗号化トンネルの開設は、以下の手順①～③で行われる(図4参照)。

①移動端末とトンネルサーバーとは、認証を行う(2-a)。

②暗号鍵のネゴシエーションを行う(2-b)。

③暗号化トンネルを開設する(2-c)。

【0005】また、一般に、暗号解読にかかる所要時間は、単位時間当たりの暗号化試行回数によって決まるため、暗号化試行速度の速い暗号ほど短時間で解読されやすい傾向がある。図5は、暗号化アルゴリズムの特性(強度・速度)とネットワークとの関係を示す図表である。この表に示すように、専用線を介した接続の場合、及び、構内ネットワークを介した接続の場合には、高い安全性は要求されないが、上記専用線や上記構内ネット

ワークが有する高い伝送速度を低下させないためにも、高速度の暗号化アルゴリズムが要求される。一方、インターネットを介した接続の場合には、伝送路（インターネット）自体の伝送速度が低いと考えられるため、高速度の暗号化アルゴリズムは要求されないが、高い安全性が要求される。

【0006】実際に現在市販されているVPNシステムとしては、（１）主に構内ネットワークにおいて使用されることを念頭におき、簡易暗号を使用しているシステム、（２）OCN等の商用インターネットサービスにおいて使用されることを念頭におき、強い暗号を使用しているシステムなどがある。上記（１）の一例としては、Logical Office（谷本他、"ロジカルオフィスサービス"、NTT R&D, Vol.45 No.10 1996年）がある。また、上記（２）の一例としては、DEC、NTT-AT社製 Altavista tunnel がある。

【0007】

【発明が解決しようとする課題】ところで、近年標準化の進展が著しい無線LANの新しい利用形態として、異種ネットワーク間にまたがって、移動しながら継続した通信を行っていく通信形態が現実のものとなってきている。該利用形態の一例としては、図3に示すように、移動端末の移動に伴って、通信を介するアクセスネットワークをアクセスネットワークCからアクセスネットワークBに変更することが考えられる。このような利用形態においては、移動端末とホームネットワークとの間における暗号化トンネルが様々な通信経路を経由することになる。

【0008】そのため、従来のシステム（単一の暗号化アルゴリズムしか用意されていないシステム）では、該用意された暗号化アルゴリズムが、現在経由している通信経路に対して、必要以上に安全であるが要求される処理速度を満たしていない場合であっても、または、必要以上に高速であるが要求される安全性を満たしていない場合であっても、該用意された暗号化アルゴリズムを使用せざるを得ない、という課題があった。

【0009】この発明は、このような背景の下になされたもので、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる認証方法を提供することを目的とする。

【0010】

【課題を解決するための手段】請求項1記載の発明は、移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネット

ワークとの接続時に認証を行い、アクセスネットワークとの認証時に、アクセスネットワークより通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、トンネルサーバーとの認証時に、選択された暗号化アルゴリズムの種別と今回のセッションを特定しうる情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、正当性が認識されると、選択された暗号化アルゴリズムによる暗号化されたVPN通信を開始することを特徴とする。請求項2記載の発明は、請求項1記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする。請求項3記載の発明は、請求項1記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする。請求項4記載の発明は、移動端末、アクセスネットワーク、中継ネットワーク、ホームネットワーク及びホームネットワーク内のトンネルサーバーから構成され、移動端末は、アクセスネットワークと中継ネットワークとを経由して、トンネルサーバーとの間で認証を行い、移動端末とトンネルサーバーとの間で暗号化トンネルを開設して通信を行う通信システムの認証方法において、移動端末は、アクセスネットワークとの接続時に認証を行い、トンネルサーバーとの認証時に、今回のセッションを特定しうる情報とアクセスネットワークとの認証時にアクセスネットワークより通知されたネットワーク情報とを、自分の署名鍵で署名して送出し、トンネルサーバーは、前記署名を検証し、移動端末より通知された今回のセッションを特定しうる情報とトンネルサーバーが管理している今回のセッションを特定しうる情報との照合結果に基づいて、移動端末の正当性を判定し、正当性が認識されると、移動端末より通知されたネットワーク情報に基づいて、必要な暗号の強度を判断して、暗号化アルゴリズムを選択し、選択された暗号化アルゴリズムによる暗号化されたVPN通信を開始することを特徴とする。請求項5記載の発明は、請求項4記載の認証方法において、前記今回のセッションを特定しうる情報として、移動端末の外部からのアクセス回数を用いることを特徴とする。請求項6記載の発明は、請求項4記載の認証方法において、前記今回のセッションを特定しうる情報として、セッションの行われた時刻情報を用いることを特徴とする。

【0011】

【発明の実施の形態】§1. 概要

本発明は、アクセスネットワークへの接続時に、移動端末とアクセスネットワークとが相互認証を行い、該アクセスネットワークに関する情報（ネットワークアドレ

ス、運用機関の情報)を得て、該情報に基づいて、必要な強度・速度の暗号化アルゴリズムを選択することを、最も主要な特徴とする。移動端末が異種ネットワーク間をまたがる移動をしながら、各時点で最も適切な暗号化アルゴリズムを選択して通信を行える点が、従来技術とは異なる。本発明によると、接続するネットワークに応じて、求められる安全性・速度を判断して、適切な暗号化アルゴリズムを選択することが可能であり、特に、無線LAN等の高度移動通信システムにおいて、常に自分のオフィス環境にアクセスし続けることを可能とする効果が得られる。

#### 【0012】§2. 第1実施形態

以下、図面を参照して、この発明の第1実施形態について説明する。なお、本実施形態は請求項2に対応するが、以下の説明において、「回数情報」を「時刻情報」と置き換えることによって請求項3に対応する説明となり、また、「回数情報」を「今回のセッションを特定しうる情報」と置き換えることによって請求項1に対応する説明となる。

【0013】図1は、この発明の第1実施形態による認証方法の一例を示すシーケンス図である。この図では、初期状態として、図3のように、「移動端末が、アクセスネットワークCを介して、ホームネットワークAとVPN暗号化トンネルを開設し、通信を行っている」場合を考える。

【0014】この初期状態において、移動端末が図3のように移動すると、通信に使用されるアクセスネットワークは、アクセスネットワークCからアクセスネットワークBに切り替わる。アクセスネットワークBに切り替わると、移動端末とアクセスネットワークBとは、公開鍵証明書を相互認証する。

【0015】移動端末は、アクセスネットワークBとの相互認証時に、アクセスネットワークBの証明書中のネットワーク情報に基づいて、アクセスネットワークBに適した暗号化アルゴリズムを選択する。

【0016】移動端末は、選択された暗号化アルゴリズムの種別を示す暗号化アルゴリズム選択メッセージに対して、該移動端末固有の署名鍵で署名し、署名された暗号化アルゴリズム選択メッセージを、ホームネットワークAのVPNの終端ノード(トンネルサーバー)に送出する。

【0017】このとき、移動端末は、(この署名された暗号化アルゴリズム選択メッセージを解析することによって求められる)上記署名鍵がアクセスネットワークBによって流用されることを防がなくてはならない。そこで、移動端末は、外部からホームネットワークAにアクセスした回数を示す回数情報を、被署名文(即ち、暗号化アルゴリズム選択メッセージ)に組み込み、この回数情報が組み込まれた暗号化アルゴリズム選択メッセージに対して署名する。これによると、アクセスネットワー

クBは回数情報を偽造できないので、署名鍵を解析・流用することも不可能となる。

【0018】回数情報が組み込まれた後に署名された暗号化アルゴリズム選択メッセージを受信すると、ホームネットワークAは、該受信内容から回数情報(即ち、移動端末が管理している回数情報、以下、「移動端末側回数情報」と称する)を取り出し、該移動端末側回数情報を、移動端末からホームネットワークAへのアクセスに関してホームネットワークAが管理している回数情報(以下、「ホームネットワーク側回数情報」と称する)と照合する。

【0019】もし、移動端末側回数情報とホームネットワーク側回数情報とが一致しないならば、ホームネットワークAは、移動端末との接続を拒否し、処理は終了する。一方、移動端末側回数情報とホームネットワーク側回数情報とが一致するならば、ホームネットワークAは、ホームネットワーク側回数情報(が示す回数)を1増やす。

【0020】ホームネットワークAは、回数情報が組み込まれた後に署名された暗号化アルゴリズム選択メッセージから暗号化アルゴリズム選択メッセージを取り出し、該暗号化アルゴリズム選択メッセージが示す種別の暗号化アルゴリズム(即ち、移動端末によって選択された暗号化アルゴリズム)に基づいて、VPN暗号化トンネルを開設する。最後に、移動端末は、移動端末側回数情報(が示す回数)を1増やす。以上で、処理は終了する。

【0021】上記の認証方法によれば、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる。

#### 【0022】§3. 第2実施形態

以下、図面を参照して、この発明の第2実施形態について説明する。なお、本実施形態は請求項5に対応するが、以下の説明において、「回数情報」を「時刻情報」と置き換えることによって請求項6に対応する説明となり、また、「回数情報」を「今回のセッションを特定しうる情報」と置き換えることによって請求項4に対応する説明となる。

【0023】図2は、この発明の第2実施形態による認証方法の一例を示すシーケンス図である。この図でも、初期状態として、図3のように、「移動端末が、アクセスネットワークCを介して、ホームネットワークAとVPN暗号化トンネルを開設し、通信を行っている」場合を考える。

【0024】この初期状態において、移動端末が図3のように移動すると、通信に使用されるアクセスネットワークは、アクセスネットワークCからアクセスネットワークBに切り替わる。アクセスネットワークBに切り替わると、移動端末とアクセスネットワークBとは、公開

鍵証明書を相互認証する。

【0025】移動端末は、アクセスネットワークBとの相互認証時に、アクセスネットワークBの証明書中のネットワーク情報に対して、該移動端末固有の署名鍵で署名し、署名されたネットワーク情報を、ホームネットワークAのVPNの終端ノード（トンネルサーバー）に送出する。

【0026】このとき、移動端末は、（この署名されたネットワーク情報を解析することによって求められる）上記署名鍵がアクセスネットワークBによって流用されることを防がなくてはならない。そこで、移動端末は、外部からホームネットワークAにアクセスした回数を示す回数情報を、被署名文（即ち、上記ネットワーク情報）に組み込み、この回数情報が組み込まれたネットワーク情報に対して署名する。これによると、アクセスネットワークBは回数情報を偽造できないので、署名鍵を解析・流用することも不可能となる。

【0027】回数情報が組み込まれた後に署名されたネットワーク情報を受信すると、ホームネットワークAは、該受信内容から回数情報（即ち、移動端末側回数情報）を取り出し、該移動端末側回数情報を、移動端末からホームネットワークAへのアクセスに関してホームネットワークAが管理している回数情報（即ち、ホームネットワーク側回数情報）と照合する。

【0028】もし、移動端末側回数情報とホームネットワーク側回数情報とが一致しないならば、ホームネットワークAは、移動端末との接続を拒否し、処理は終了する。一方、移動端末側回数情報とホームネットワーク側回数情報とが一致するならば、ホームネットワークAは、ホームネットワーク側回数情報（が示す回数）を1増やす。

【0029】ホームネットワークAは、回数情報が組み込まれた後に署名されたネットワーク情報からネットワーク情報を取り出し、該ネットワーク情報に基づいて、アクセスネットワークBに適した暗号化アルゴリズムを選択する。ホームネットワークAは、該選択された暗号化アルゴリズムに基づいて、VPN暗号化トンネルを開設する。最後に、移動端末は、移動端末側回数情報（が

示す回数）を1増やす。以上で、処理は終了する。

【0030】上記の認証方法によれば、異種ネットワーク間でシームレス移動を行いながらホームネットワークへのアクセスを継続しても、必要な強度・速度の暗号化アルゴリズムを適切に選択することができる。

【0031】§4. 捕捉

以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計の変更等があってもこの発明に含まれる。

【0032】

【発明の効果】以上説明したように、この発明によれば、アクセスネットワークに関するネットワーク情報に基づいて暗号化アルゴリズムを選択することができるので、必要な安全性と処理速度とを備えた暗号化アルゴリズムを適切に選択することができる。特に、無線LANを用いたモバイルコンピューティングにおいては、本発明により、シームレスに異種ネットワーク間を移動することができるようになる。また、「従来の技術」の項で説明したようなシステム（構内ネットワーク向けシステムと商用インターネット向けシステム）の2つを、ユーザーに購入させる必要がなくなるため、システムベンダーとしては、スケールメリットを享受できる。

【図面の簡単な説明】

【図1】 この発明の第1実施形態による認証方法の一例を示すシーケンス図である。

【図2】 この発明の第2実施形態による認証方法の一例を示すシーケンス図である。

【図3】 VPNを開設して通信を行うシステムの概要例を示す説明図である。

【図4】 暗号化トンネルを開設する手順の一例を示すシーケンス図である。

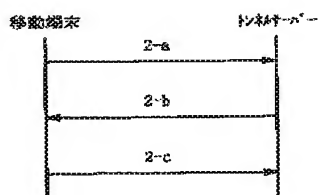
【図5】 暗号化アルゴリズムの特性（強度・速度）とネットワークとの関係を示す図表である。

【符号の説明】

A……ホームネットワーク

B, C……アクセスネットワーク

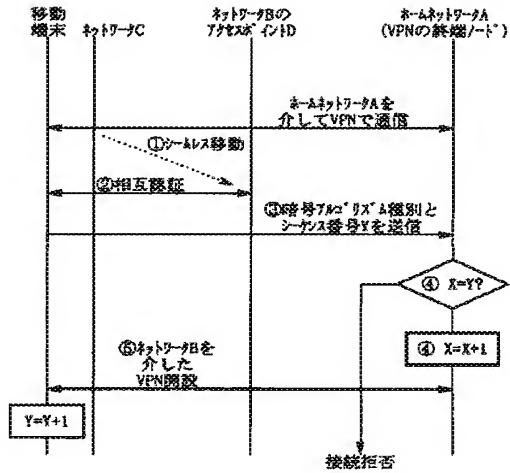
【図4】



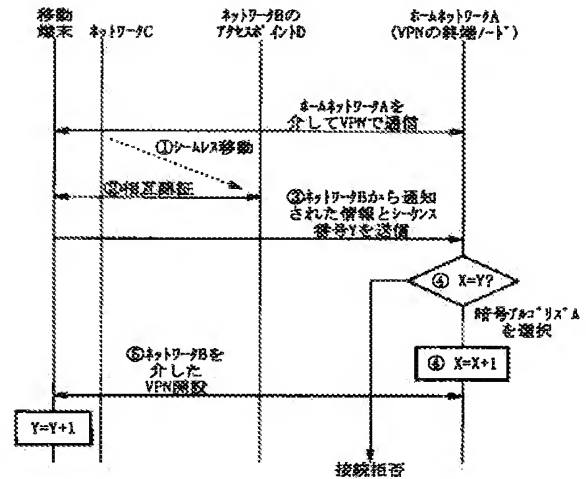
【図5】

	構内/専用線接続	インターネットを介した接続
強い暗号 (遅い暗号)	適していない。	適している。
弱い暗号 (早い暗号)	適している。	適していない。

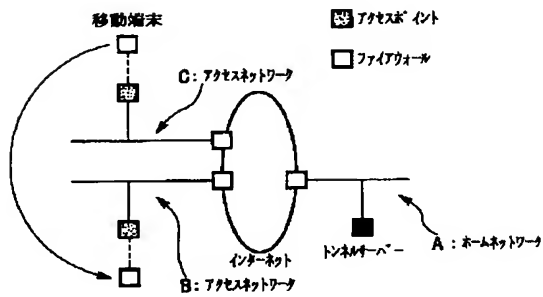
【図1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

H 0 4 L 12/66

識別記号

F I

ターム (参考)

(72) 発明者 守倉 正博

東京都新宿区西新宿三丁目19番2号 日本  
電信電話株式会社内

F ターム (参考) 5J104 AA07 AA35 AA36 KA02 KA10

NA38 PA01 PA07

5K030 GA15 JT09

5K033 AA08 DA19

9A001 CC05 CC06 EE03 JJ27 LL03